REMARKS

The Specification has been amended. Claims 1, 3, 9 - 11, 15, 22, 24, 26 - 27, 32, 34 - 35, 37, 40, 45, and 54 - 56 have been amended to more clearly specify the subject matter of Applicants' claimed invention. No new matter has been introduced with these amendments, all of which are supported in the specification as originally filed. Claims 1, 3 - 15, 22, 24 - 27, 32, 34 - 40, and 45 - 58 remain in the application.

I. Objection to the Claims

Paragraph 3 of the Office Action dated July 26, 2006 (hereinafter, "the Office Action") states that Claims 1, 22, and 32 are objected to because of informalities. Appropriate amendments have been provided herein, and the Examiner is respectfully requested to withdraw this objection.

II. Rejection under 35 U.S.C. §112, second paragraph

Paragraph 6 of the Office Action states that Claims 1, 3 - 15, 22, 24 - 27, 32, 34 - 40 and 45 - 58 are rejected under 35 U.S.C. §112, second paragraph, as being indefinite. Appropriate corrections have been provided herein, and the Examiner is respectfully requested to withdraw this rejection.

III. Rejection Under 35 U.S.C. §102(e)

Paragraph 8 of the Office Action states that Claims 1, 3 - 15, 22, 24 - 27, 32, 34 - 40,

and 45 - 58 are rejected under 35 U.S.C. §102(e) as being anticipated by U. S. Patent 6,279,113 to Vaidya. This rejection is respectfully traversed.

Applicants have amended their independent Claims 1, 22, and 32 to more clearly specify limitations of their claimed invention. Applicants' independent Claim 1 specifies limitations of:

- "defining a plurality of intrusion suspicion levels ..." (Claim 1, lines 3 - 5, emphasis added);
- "associating one of the defined intrusion suspicion levels with each of the sets [of conditions], wherein the associated intrusion level indicates how suspicious is an inbound communication matching each condition in the set" (Claim 1, lines 8 - 10, emphasis added);
- "defining a plurality of sensitivity levels for filtering the inbound communications as potential intrusion events when performing the intrusion detection processing, each of the defined sensitivity levels usable for a different level of filtering of the inbound communications" (Claim 1, lines 11 - 13, emphasis added); and
- "if [any of the sets is matched for the particular inbound communication], filtering the particular inbound communication by using a currently-applicable one of the defined sensitivity levels, in concert with the intrusion suspicion level associated with the [matched] set ..." (Claim 1, lines 18 - 21, emphasis added).

Independent Claims 22 and 32 specify similar limitations. Applicants respectfully submit that Vaidya does not teach, nor suggest, (at least) the above-underlined limitations. The Office Action makes a general reference to Vaidya, col. 7, line 52 - col. 8, line 39 for teaching all of the limitations of Applicants' independent Claim 1. The Office Action further states, with regard to this cited text (emphasis added),

> noting that higher sensitivity to certain actions with different levels of suspicion, depending on the previous conditions met in a "sequential" profile, or on the timing and count values in a "timer/counter" profile, will make detection of an attack more likely; for example, if a first condition has been met in a sequential profile, column 7, lines 52 - 67, then the sensitivity level is raised for the next packets, and if those packets have an appropriate suspicion level, column 8 lines 1 - 15, then an intrusion event is detected; noting further that there are a plurality of intrusion and sensitivity levels defined depending on the profiles used).

To suggest that Vaidya's references to sequential profiles or timer/counter-oriented profiles teach the precise claim language of Applicants' independent claims violates the holding of the Federal Circuit in ***Motorola, Inc. v. Interdigital Technology Corp.***, 43 USPQ 2d 1481, 1490 (Fed. Cir. 1997), which stated

> For a prior art reference to anticipate a claim, the reference must disclose each and every element of the claim with sufficient clarity to prove its existence in the prior art. *See In re Spada*, 911 F.2d 705, 708, 15 USPQ 2d 1655, 1657 (Fed. Cir. 1990) ("[T]he [prior art] reference must describe the applicant's claimed invention sufficiently to have placed a person of ordinary skill in the field of the invention in possession of it." (citations omitted)). Although this disclosure requirement presupposes the knowledge of one skilled in the art of the claimed invention, that presumed knowledge does not grant a license to read into the prior art reference teachings that are not there. (emphasis added)

The Office Action states, on p 3, lines 7 - 17, that Applicants' response dated April 4, 2006 fails to comply with 37 C.F.R. 1.111(b) because it does "not provide any evidence in support of" an "allegation" that Vaidya fails to teach limitations of Applicants' claimed invention. Because it appears impossible to provide "evidence" as to *where* something is not taught, Applicants will set out a discussion herein of what *is* taught by Vaidya, and will contrast this to their claimed invention.

With regard to Applicants' claimed "intrusion suspicion levels", Applicants respectfully submit that there is simply no discussion, nor any suggestion, in Vaidya of "defining a plurality of intrusion suspicion levels ..." (Claim 1, lines 3 - 5, emphasis added) or "associating one of the *defined* intrusion suspicion levels with each of the sets [of conditions], wherein the associated intrusion suspicion level indicates how suspicious is an inbound communication matching each condition in the set" (Claim 1, lines 8 - 10, emphasis added). The Office Action's analysis of intrusion suspicion levels (with regard to Claim 1) will now be discussed to demonstrate that this teaching is missing from Vaidya.

The Office Action first refers to "different levels of suspicion" in paragraph 8, lines 10 - 13, inferring that there are "certain actions with different levels of suspicion" in Vaidya. The Examiner is respectfully requested to identify where in Vaidya this statement is supported, as Applicants respectfully submit that Vaidya simply teaches that each packet is inspected in turn (and as is obvious, some of those packets may match conditions while others do not) with no

discussion, nor any suggestion, of having the "different levels of suspicion" asserted in the Office Action. See, for example,

- Abstract, lines 12 - 14, indicating that when a data packet is detected, its packet information is extracted; there is no discussion therein of any "different level of suspicion";
- **Fig. 3**, reference numbers **58 - 66**, which discuss a high-level view of monitoring data (**58**) and executing instructions (**62**) from an attack signature profile (**60**) to determine if an intrusion has been detected (**64**); however, there is no suggestion therein of any different "suspicion levels" involved in this processing;
- **Fig. 8**, where the format of an attack signature profile **198** is depicted, fails to show any "associating" of a defined intrusion suspicion level therewith;
- **Fig. 9**, depicting high-level processing of the various types of attack signature profiles, fails to indicate any type of "different levels of suspicion";
- **Fig. 10**, depicting the processing of a sequential attack signature profile, fails to show any kind of processing for "different levels of suspicion", and instead, simply goes through the sequential expressions in order;
- **Fig. 12**, depicting the processing of a timer/counter attack signature profile, has no suggestion of any processing for "different levels of suspicion" and instead, simply adds a current time stamp (**186**) and updates a counter (**188**) if a match is found; notably, this processing occurs for every matching packet from the first through the last, without any kind of "different levels of suspicion";

- col. 3, lines 12 - 26 describe Vaidya's attack signature profiles, but there is no mention therein of any "different levels of suspicion" that might be associated with the profiles or with the packets they operate against;
- col. 3, lines 35 - 39 discuss information that is associated with the attack signature profiles; however, this information is an indication of the network objects to which the signature profile corresponds (see also col. 6, lines 37 - 40, where this is discussed with reference to **Figs. 2 - 3**), which is distinct from Applicants' associating of intrusion suspicion levels with sets of conditions;
- col. 3, lines 40 - 48 discuss monitoring for data packets and checking for intrusions, without any suggestion of any "different levels of suspicion" involved therewith; instead, the signature profiles corresponding to the network object to which the packet is addressed (i.e., according to the association data discussed at col. 3, lines 35 - 39) are those that will be processed;
- col. 4, lines 8 - 18 discuss processing of sequential attack signature profiles, but there is no discussion therein of any "different levels of suspicion"; rather, this text describes sequential processing for multiple events over a portion of an application session and maintaining an indication of which events have occurred (i.e., matched);
- col. 4, lines 19 - 27 discuss processing of timer/counter attack signature profiles, stating that "The instruction [from the profile] is executed on each packet ..." (emphasis added); in other words, as stated above with reference to **Fig. 12**, Vaidya teaches that all of these packets are treated equally, in contrast

to the assertion in the Office Action that they have "different levels of suspicion";

- col. 6, lines 3 - 7 discuss the above-mentioned associations "between network objects and attack signature profile sets", and as has been discussed above, this is clearly different from Applicants' claimed "associating" of an intrusion suspicion level with a set of conditions (Claim 1, lines 8 - 10);
- col. 6, lines 7 - 14 discuss checking of packets against the attack signature profiles, but as has been stated herein, there is no suggestion therein of any "different levels of suspicion" associated with the packets or with the profiles;
- col. 6, line 57 - col. 7, line 2 discusses monitoring data packets and accessing the attack signature profiles corresponding to the network object to which the packets are addressed -- again, without any suggestion of handling "different suspicion levels";
- col. 7, lines 4 - 11 state that when an evaluated data packet is not associated with a network intrusion, "the data collector continues to monitor data" (notably, with no change in any "suspicion levels") whereas upon detecting a network intrusion, "the reaction module is notified" (and again, there is no mention or any suggestion of a "different suspicion level" resulting from detecting this intrusion, in contrast to the assertion in the Office Action);
- col. 7, lines 12 - 31 explain that information extracted from packet headers is used to determine which attack signature profiles to use when evaluating a packet, and this extracted information is described in terms of addressing

information for the packet destination (in accordance with the above-discussed "association" between profiles and network objects for which those profiles may be used); again, there is no mention of any "different suspicion levels";

- col. 7, lines 36 - 51 describe processing for a "simple" attack signature profile, and as the Office Action makes no assertions regarding this type of profile, it will not be discussed further herein;
- col. 7, line 52 - col. 8, line 15 describes processing for a sequential attack signature profile; this text is described in more detail, below, with reference to the Office Action's second reference to "suspicion level";
- col. 8, lines 16 - 39 describe processing for a timer/counter attack signature profile, stating that the instructions associated with a "single expression" (i.e., as specified in the profile) are executed on every data packet of a particular session (as stated in col. 8, lines 16 - 18 and lines 24 - 25); this identical treatment of every data packet in the session teaches away from the assertion in the Office Action that there is some type of "different level of suspicion" that depends on "the timing and count values" in the profile (Office Action, paragraph 8, lines 11 - 12);
- col. 9, lines 3 - 20 discuss checking a state cache **44** to determine whether information for the current application session is stored therein, and if so, that information "might contain a record of timer/counter expressions executed on packets" (col. 9, lines 11 - 18) or it might contain information about the expressions matched in a sequential attack signature profile (col. 9, lines 19 -

20); however, there is no discussion therein of "different levels of suspicion";

- col. 9, lines 27 - 46 describe searching the instruction cache **42** to determine whether attack signature profiles for the destination network object (i.e., the network object identified using "the server IP address and the application information") are stored therein, and if not, then the corresponding profiles are located and imported; again, there is no suggestion of any "different suspicion levels" associated with the profiles;
- col. 9, lines 47 - 61 describe how an attack signature profile "can be represented"; however, none of the described information suggests "different suspicion levels";
- col. 9, line 62 - col. 10, line 16 describes a "simple" attack signature profile and a timer/counter attack signature profile, again without any suggestion of "different suspicion levels" associated with these profiles or the packets they will be executed against; instead, col. 9, line 66 - col. 10, line 3 states that the timer/counter profiles are "executed sequentially on each data packet associated with an application session ...";
- col. 10, lines 17 - 21 discuss the sequential profiles, stating that the multiple expressions "are sequentially executed on [each of the] successively transmitted data packets" of the session -- without any suggestion of different suspicion levels;
- col. 10, lines 22 - 44 set out a "loose" BNR grammar for an attack signature, and Applicants note that this grammar fails to specify any type of suspicion

levels associated with these profiles;

- col. 10, line 46 - col. 11, line 4 provides a high-level discussion of checking the attribute associated with an attack signature profile for a particular network object, and invoking corresponding processing for that attribute (which may be, for example, a sequential attribute or a timer/counter-based attribute);
- col. 11, lines 5 - 15 describe detection of an intrusion, stating that "in step **138** the reaction module **38** is notified" whereas if an intrusion is not detected and there are still attack profiles in the instruction cache, then the virtual processor **36** "accesses the next attack signature"; or, if there are no more attack profiles to be executed, then the next packet in the queue **48** is obtained for processing -- but again, there is no suggestion of any "different levels of suspicion";
- col. 11, lines 16 - 51 describe processing of sequential attack signature profiles in more detail, stating that the multiple expressions therein are "sequentially evaluated" (col. 11, lines 20 - 21) and stating that the expressions need not match consecutive data packets but must just proceed in order (col. 11, lines 45 - 51); again, there is no discussion of any "different levels of suspicion" associated therewith;
- col. 11, lines 52 - 65 describes processing that follows executing an "expression instruction" from a sequential profile, stating conditions under which a "true" or "false" value may be returned to the invoking logic, but failing to teach or suggest that there is any type of "different level of suspicion" associated with these various returned values;

- col. 12, lines 11 - 33 describe processing of timer/counter attack signature profiles in more detail, stating that the expression therein is evaluated to determine if it matches the packet being analyzed (col. 12, lines 23 - 25) and if it does not, then a value of "false" is returned (col. 12, lines 25 - 26) whereas when it does match, then a value of "true" is returned and the time stamp and counter are updated accordingly (col. 12, lines 26 - 33); and
- col. 12, lines 33 - 41 describe processing that follows a determination that the expression in the timer/counter profile matched the data packet, and discusses conditions under which a "true" or "false" value may be returned to the invoking logic, but fails to teach or suggest that there is any type of "different level of suspicion" associated with these various returned values.

As can be seen by the above, none of the text in Vaidya actually teaches or suggests "different levels of suspicion", in contrast to the assertion in paragraph 8, line 11 of the Office Action. Accordingly, Applicants respectfully submit that the rejection is based on prohibited hindsight reasoning where that which the inventor has invented is impermissibly used against him. See ***W.L. Gore & Associates, Inc. v. Garlock, Inc.***, 220 USPQ 303, 312–13 (Fed. Cir. 1983), ***cert. denied***, 469 U.S. 851 (1984), where the Federal Circuit held

> To imbue one of ordinary skill in the art with knowledge of the invention in suit, when no prior art reference or references of record convey or suggest that knowledge, is to fall victim to the insidious effect of a hindsight syndrome wherein that which only the inventor taught is used against its teacher.

Furthermore, Applicants respectfully note that their claim language does not specify that "certain actions" have different suspicion levels, in contrast to the language in paragraph 8, lines 10 - 11 of the Office Action. Rather, Applicants' claim language specifies that an intrusion suspicion level is associated with a defined set of conditions (Claim 1, lines 6 - 10). As has been established above, Vaidya's profiles (which may be considered analogous to Applicants' sets of conditions) do not have suspicion levels associated therewith.

A second reference to "suspicion level" is found on page 8, line 1 of the Office Action, which states that "[those] packets have an appropriate suspicion level", citing col. 8, lines 1 - 15. Applicants respectfully submit that the cited text discusses only evaluating a sequence of packets to determine if the multiple expressions in a sequential attack signature profile have been met, and this does not teach or suggest that packets have a suspicion level (as has been discussed above).

Referring next to Applicants' claimed "sensitivity levels", Applicants respectfully submit that there is simply no discussion, nor any suggestion, in Vaidya of "defining a plurality of sensitivity levels for filtering the inbound communications ..., each of the defined sensitivity levels usable for a different level of filtering of the inbound communications" (Claim 1, lines 11 - 13, emphasis added) or "filtering the particular inbound communication by using a currently-applicable one of the *defined* sensitivity levels, in concert with the intrusion suspicion level *associated with* the [matched] set [of conditions] ... to determine if the particular inbound communication should be treated as an intrusion event" (Claim 1, lines 18 - 21, emphasis

added). The Office Action's analysis of sensitivity levels (with regard to Claim 1) will now be discussed to demonstrate that this teaching is missing from Vaidya.

The Office Action first refers to sensitivity levels in paragraph 8, lines 10 - 11, using the term "higher sensitivity to certain actions ...", and inferring that this higher sensitivity arises because of "previous conditions met" in a sequential profile or "on the timing and count values" in a timer/counter profile. Paragraph 8, lines 13 - 15 of the Office Action then refer to sensitivity levels again, stating that "if a first condition has been met ... then the sensitivity level is raised for the next packets", citing col. 7, lines 52 - 67 of Vaidya. However, Applicants respectfully submit that for both of these statements in paragraph 8, the Examiner is using prohibited hindsight reasoning to read these teachings into Vaidya, as the statements in the cited text make no mention of "higher sensitivity to certain actions" or "raising" any kind of "sensitivity level".

Furthermore, with regard to the Office Action assertion that some kind of "higher sensitivity" occurs in Vaidya's approach, upon a careful reading of Vaidya, it can be seen that it is possible to meet all of the multiple expressions of a sequential profile with a single packet. See, for example, col. 7, lines 52 - 55, which introduce an example where a sequential profile includes a first expression "is source address user Z?" and a second expression "is user Z attempting to access file A?". Col. 7, lines 55 - 58 then explain that instructions associated with the first expression are evaluated with regard to a first packet; for this particular example, the first expression is matched -- that is, this is a packet with source address of user Z. Lines

58 - 60 of col. 7 then state "However, if this first packet does not include information that user Z is attempting to access file A in application X, a subsequent packet ... will have to be analyzed ...". By implication, an opposite outcome is also possible where the first packet does "include information that user Z is attempting to access file A in application X", and under this opposite outcome, it would not be necessary to analyze "a subsequent packet" because both of the expressions would already be met. See **Fig. 10**, which provides logic for sequential attack signature profile handling (per col. 11, lines 16 - 17), and in particular, the tests at **154** and **158**. If both of these tests have a positive result when processing a single packet, then at **164**, "true" is returned to the invoking logic -- namely, **134** in **Fig. 9** -- to "indicate that a network intrusion has been detected" (see col. 11, lines 52 - 65, and in particular, lines 62 - 65 thereof). Control then reaches **136** of **Fig. 9**, which will also have a positive result (col. 11, lines 5 - 7), causing **138** of **Fig. 9** to notify a "reaction module" (col. 11, lines 7 - 8).

It is clear that in the scenario where a single packet meets all of the expressions within a sequential attack signature profile, there is no type of higher sensitivity to any subsequent packets (because no additional packets are needed), in contrast to the assertions on lines 10 - 12 and lines 14 - 15 of paragraph 8 of the Office Action. And with regard to a scenario in which multiple packets are evaluated before meeting all of the expressions, refer to the above-presented discussion of Vaidya's text: there is, in fact, no teaching or suggestion therein of any "higher sensitivity" occurring during this processing.

Applicants also note that page 8, lines 2 - 3 of the Office Action state "there are a

plurality of intrusion and sensitivity levels defined depending on the profiles used". The Examiner is respectfully requested to identify where in Vaidya this is stated, as Applicants respectfully submit that this assertion is based only on impermissible hindsight reasoning.

Applicants' independent Claims 22 and 32 specify similar limitations to those which have been discussed herein for independent Claim 1. As has been demonstrated, Vaidya does not teach, nor suggest, all of the limitations in these claims. Accordingly, Applicants' independent Claims 1, 22, and 32 are deemed patentable over Vaidya. In view of the patentability of the independent claims, Applicants respectfully submit that their dependent Claims 3 - 15, 24 - 27, 34 - 40, and 45 - 58 are also patentable over Vaidya.

Furthermore, Applicants respectfully submit that the Office Action fails to make out a *prima facie* case of anticipation to a number of their dependent claims. Dependent Claim 15, for example, specifies limitations that pertain to a "stored mapping". When analyzing this claim on page 9 of the Office Action, a citation to col. 5, lines 27 - 33 is provided, noting that Vaidya teaches "a plurality of profiles are defined". This is irrelevant to the stored mapping specified in Claim 15, which maps "defined sensitivity levels" and "defined intrusion suspicion levels" (Claim 15, lines 4 - 5). This analysis of Claim 15 also cites col. 7, line 52 - col. 8, line 39. However, as has been discussed, this text states that multiple packets are evaluated to determine if a profile is matched; this does not teach, or suggest, a "stored mapping" as claimed in Claim 15.

Applicants also note that the Office Action fails to provide any citations for the limitations in dependent Claim 48 (pertaining to a "deny filter") and dependent Claim 53 (pertaining to "establish[ing] baselines"). Without more, these claims are deemed patentable over Vaidya.

In view of the above, the Examiner is respectfully requested to withdraw the §102 rejection of all claims as currently presented.

IV. Conclusion

In conclusion, Applicants respectfully request reconsideration of the pending rejected claims, withdrawal of all presently outstanding objections and rejections, and allowance of all remaining claims at an early date.

Respectfully submitted,

/Marcia L. Doubet/ /#40,999/

Marcia L. Doubet
Attorney for Applicants
Reg. No. 40,999

Customer Number for Correspondence: 43168
Phone: 407-343-7586
Fax: 407-343-7587